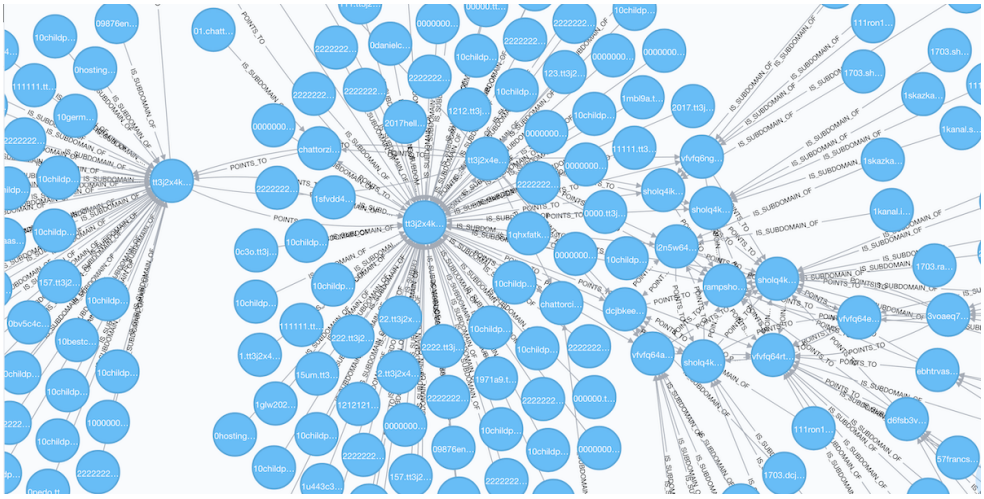
# Daniel of the Darknet goes Dark

## This Week, 6,500 Hidden Services were Ousted from the Darknet

The name Daniel Winzen may not mean much to the ordinary internet user, but on the darknet *@daniel* is the legendary nickname for the individual known for offering free anonymous web hosting, chat, e-mail, and XMPP/Jabber services on Tor for the last 5 years and perhaps longer. He started out humbly – installing a small number of Tor-based hidden services, or websites, on a Raspberry PI 2 – but over the years expanded his presence to hosting upwards of 7,000 hidden services per month for darknet users across Tor and I2P. That is, until last week.

Shortly after 10:00pm UTC on the 15th of November 2018, Daniel Winzen's server was breached, databases accessed, and accounts deleted, including the root, or administrator account, rendering his services unusable. In less than three hours, the intruders deleted SQL databases for his chat, onion-link list, and hit counter. Hackers initially accessed the main phpMyAdmin and adminer panels using the correct hosting management password, inferring the password may have been harvested via phishing attempt or the server was accessed by someone with access to Daniel's credentials. Daniel's popular GitHub account also experienced a failed login for his popular software repository on November 9th, which has not been determined as related as of yet.

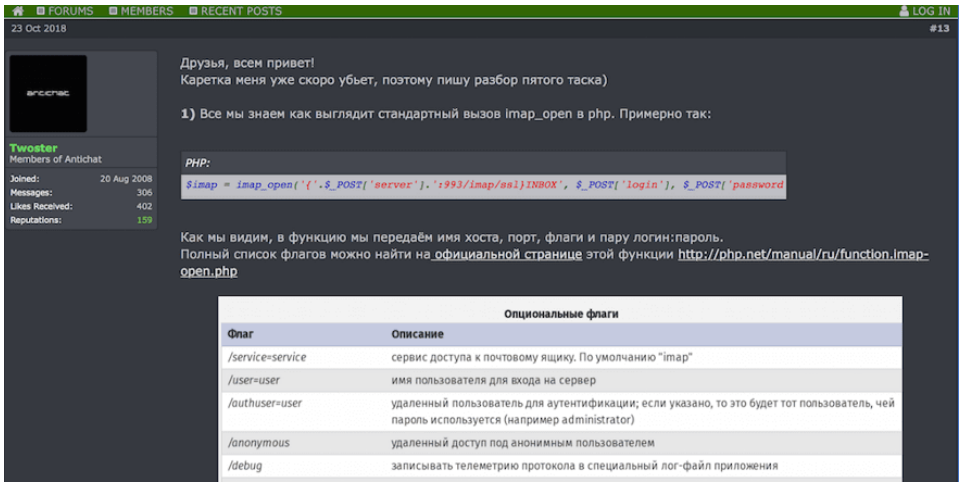
Daniel's updates on his portal indicates that this hack was a "database only" breach.



*Daniel Winzen's services link many other hidden services on Tor and i2p*

""Other than the root account, no accounts unrelated to the hosting were touched and unrelated files in /home/ weren't touched either. As of now there is no indication of further system access and I would classify this as a "database only" breach, with no direct access to the system. From the logs it is evident that both, adminer and phpmyadmin have been used to run queries on the database.""

According to updates posted to his surface net and darknet portal, Winzen is thoroughly investigating all potential vulnerabilities in his server before restoring services. He has also listed concern over a 0-day exploit, released exactly one day before the attack, in the imap_open() function of PHP that he has since patched.




*Russian Security Forum discusses exploiting imap_open() function*

## 30% of Online Domains Disappeared Overnight

Over 30% of the operational and active hidden services across Tor and I2P disappeared with the hack of Daniel's Hosting Services and over **6-Million** documents archived in DarkOwl Vision are no longer available on the darknet.

DarkOwl quantified the impact to the size of the darknet, specifically Tor, using its internal "Map the Dark" reporting, which includes statistics from darknet websites indexed over the previous 24-hour period. Our data substantiates the hosting provider's offline status, with a delta of 4,887 domains going offline between the 15th and 16th of November. DarkOwl has indexed the archives of 5,300 domains from early November and has assessed them to be services that were formerly hosted on Daniel's server.

Daniel's previous online-link list advertised that he hosted over 1,500 private hidden services whose domain URLs are unknown at this time. DarkOwl's estimated total number of domains hosted by Daniel are consistent with the 6,500 offline domains quoted by Daniel on his server portal.

- **657** of the hidden services have only title *"Site Hosted by Daniel's Hosting Service"* and contain no meaningful content worth mentioning. Darknet hidden service domain could have been used for something other than serving web content.
- **Over 4,900** of the hacked domains are in English and 54 are Russian-language hidden services. Two of the oldest hidden services are interestingly in the Portuguese language.
- **457** of the hidden services contain content related to **hacking and/or malware** development, while 136 include **drug**-specific keywords.
- **304** of the hidden services have been classified as **forums** and 148 of them are **chatrooms**.
- **109** of the hidden services contain **counterfeit** related content while 54 specifically mention **carding**-specific information.
- **Over 20** of the hidden services contain content including **weapons & explosive** related keywords.

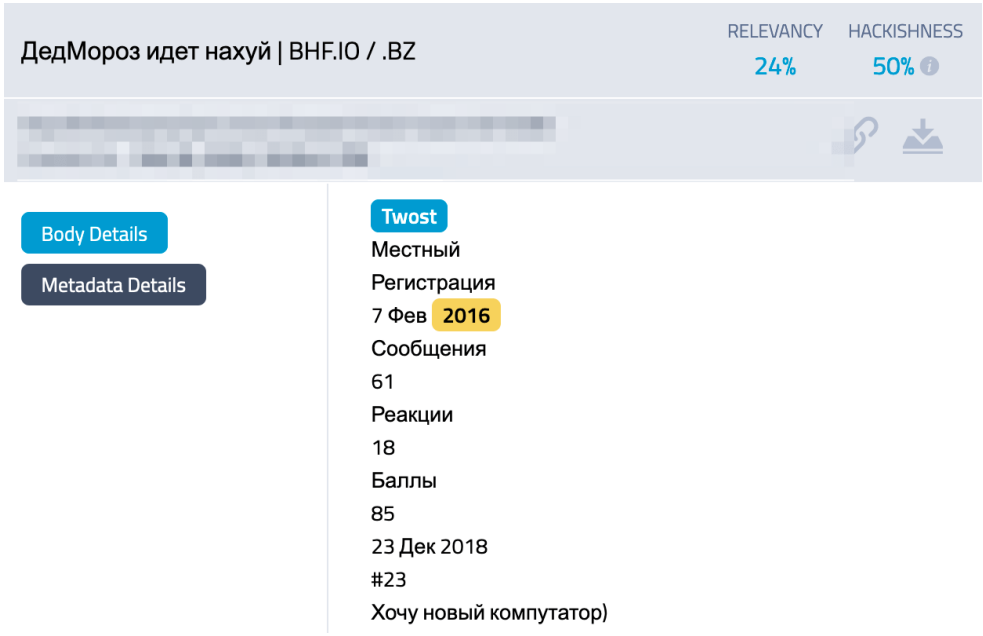
Daniel's hosting service, chatroom and online-link list have served as a pillar for the darknet community for years. For example, his online-link list is referenced by nearly 500 other hidden services, making it the second most commonly referred to directory listing (behind Fresh Onions) and providing a foundational starting point for new users navigating Tor.

Given that his services were provided free of charge and generally reliable against attack, there are mixed theories as to who could have wanted to destroy this mainstay of the anonymous online community.

## Are Russian Hackers Responsible?

In recent weeks, Russian hackers on a website called *www.antichat.com*, outlined the technical details of exploiting PHP's imap_open() function to extract password hashes for privileged

accounts, as an alternative to brute force mining. Then, on Thursday (the same day as the attack), *antichat.com* forum staff member "*Big Bear*" posted a MEGA.nz link including a PDF, titled, "*[RCE] 0-day в imap/c-client на примере PHP*" (in English: [RCE] 0-day in imap / c-client using the example of PHP) detailing the imap_open exploit. The same post identifies the authors by the nicknames *crlf* and *Twost*, the latter of whom is also known as "Aleksandr."

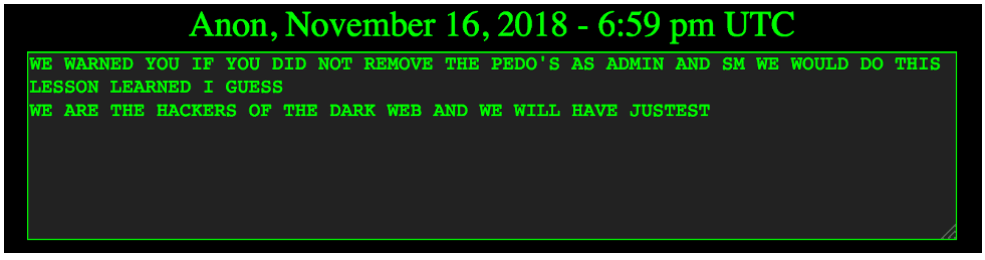



*DarkOwl Vision shows darknet mentions of the alias Twost dating back to 2016. (d17f1c43136b7d764b525ddd52442458)*

## The Anti Child-Exploitation Community

Daniel's darknet notoriety increased in 2016 when he ported Lucky Eddy's perl-CGI LE-Chat script into PHP with mySQL or PostgreSQL backend, optimizing the environment for Tor and decreasing the darknet community's reliance on Javascript, thus allowing for image sharing inside a chat platform (which is not available via XMPP and IRC) without potentially compromising posters' identities. As a result, Daniel's LE-Chat code became a popular platform for the darknet pedophilia community, and the home for many well-known Child Pornography sharing chatrooms such as Tabooless, Camp Fire, and Child Priori.

Individual "pedo-hunters" and anti-pedophilia groups have called for hacking Daniel's services using large-scale distributed denial of service (DDoS) campaigns, specifically because it was rumored that the principal administrator and some key staff members were active in pedophilia-specific chats.




*Anonymous post suggesting the hack was motivated by an anti-pedo agenda*

## A Potential Law Enforcement Operation

Daniel's Chat quietly resurfaced this past Saturday with a clean install and backup from early 2017, accompanied by a flurry of confusion over the assignments of administrator, moderators, and members. Without the comforting presence of the "regular" member database and credentials, users had no way to verify that anyone was who they said they were. Many legitimately feared that popular nicknames of members and staff had been spoofed by trolls trying to capture access to the members-only chat. One user on the darknet social media site Galaxy3 stated that @daniel re-installed the chat and that it "sounded like him," although with a caveat that everyone should be cautious.

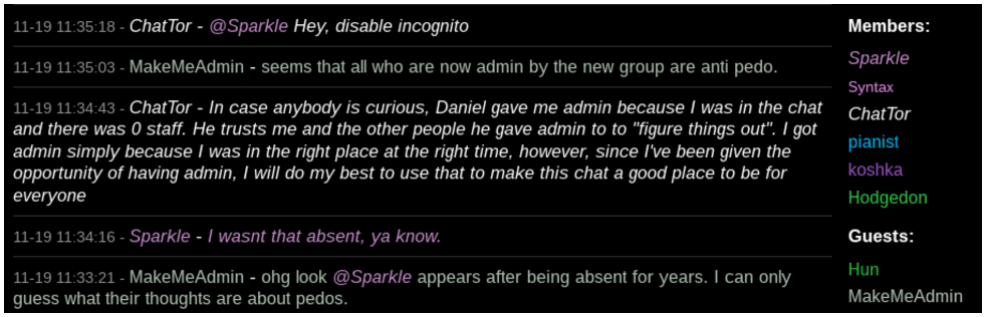
At the same time, others theorized the extreme possibility that @daniel had actually been arrested and the take-down was led by international law enforcement or the German police. Daniel's hidden services experienced extreme DDoS in the weeks preceding the hack, similar to other law enforcement-led darknet seizure operations.


*Galaxy3 Post by user ChatTor (http://galaxy3m2mn5iqtn[.]onion)*

## Anti-Syntax Club or an Inside Job

For over a year, the nickname *Syntax* has been referenced with either extreme love or extreme hate. Hundreds of trolls have posted across forums and paste sites about how this purportedly 17-year-old female teenager is responsible for taking down a number of pedophilia chatrooms and community leaders in recent years. Since early this fall, there has been an increase in the number of anti-*Syntax* trolls repeatedly calling for attacks against Daniel's services, more specifically *Syntax* and her ally *ChatTor*, since she was promoted to Super Moderator of Daniel's popular and drama-filled chatroom during the summer and accused of abusing the position.

Other members have suggested the remote possibility the attack on Daniel's was led by *Syntax* and *ChatTor* so that they could take administrative control of the chatroom, although a recent image capture from *ChatTor* states that it was simply about being at the right place at the right time.




*Capture of Le-Chat conversation debating the validity of staff with Daniel's services (http://mat32scrdvrn5o4m.onion/neo/uploads/181119/MATRIX_115636_YsP_ChatTorConfession[.]png)*

## Explore the Products

### Products

OVERVIEW
VISION UI
SEARCH API
ENTITY API
SCORE API
RANSOMWARE API
DATAFEEDS
VISION RESOURCES
API RESOURCES

### Use Cases

OVERVIEW
CYBER INSURANCE UNDERWRITING
THREAT INTELLIGENCE
DIGITAL IDENTITY PROTECTION
THIRD PARTY RISK
FRAUD PROTECTION
CRITICAL INFRASTRUCTURE
NATIONAL SECURITY

### Company

ABOUT
LEADERSHIP
PRESS RELEASES
CAREERS
SUBSCRIBE TO EMAIL
MAP THE DARK
CONTACT US




DarkOwl is a Denver-based company that provides the world's largest index of darknet content and the tools to efficiently find leaked or otherwise compromised sensitive data. We shorten the timeframe to detection of compromised data on the darknet, empowering organizations to swiftly detect security gaps and mitigate damage prior to misuse of their data.